

AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph beginning on page 17, line 24 as follows:

Figure 1 is a block diagram illustrating a structure of a public key generation apparatus according to a first embodiment ~~embodiment, corresponding to claim 1~~ of the present invention.

Please amend the paragraph beginning on page 20, line 15 as follows:

A shared key generation apparatus according to a second embodiment ~~embodiment, corresponding to Claim 5~~ of the present invention will be described.

Please amend the paragraph beginning on page 23, line 17 as follows:

A key exchange apparatus according to a third embodiment ~~embodiment, corresponding to Claim 9~~ of the present invention will be described.

Please amend the paragraph beginning on page 24, line 9 as follows:

Hereinafter, the operation of the key exchange apparatus 33 according to the third embodiment will be described.

Please amend the paragraph beginning on page 27, line 8 as follows:

A key exchange apparatus according to a fourth embodiment ~~embodiment, corresponding to Claim 13~~ of the present invention will be described.